REMARKS

The Office Action mailed March 6, 2007 has been received and reviewed. Claims 1-30 are pending. Claim 27 is rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Claims 1, 2, 4-9, 11, 13-17, 19, 21-25, and 27-29 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,918,113 to Patel ("Patel"). Claims 3, 10, 12, 18, 20, 26, and 30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Patel in view of U.S. Patent No. 6,810,525 to Safadi ("Safadi").

Rejections Under 35 U.S.C. §101

Claim 27 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter for reciting software constructs rather than the manipulation of hardware or a tangible entity. Applicants respectfully assert that claim 27 recites the steps of "opening a computer resource" and "providing a notification when the monitored usage has exceeded the user's credit" each of which requires manipulation of hardware or a tangible entity.

Discussion of the Disclosed Embodiments

The disclosed embodiments of the invention will now be discussed in comparison to the prior art. Of course, the discussion of the disclosed embodiments, and the discussion of the differences between the disclosed embodiments and the prior art subject matter, do not define the scope or interpretation of any of the claims. Instead, such discussed differences merely help the Examiner appreciate important claim distinctions discussed thereafter.

Applicants disclose, in one embodiment, a method for allowing a user at a remote computer system to access a computer resource, such as an application. A token is generated remote from the computer system, such as at a server, and is then transmitted to the user's computer system, such as by means of a smart card storing the token. The token contains encrypted user information including credit, authorization, and authentication information. The computer resource may be independently usable on the user's computer system or may be a module allowing remote access to an application or other resource stored on a server. The computer resource is encrypted such that the user may access it only upon completion of authorization and verification steps discussed below.

A request is initiated to open the encrypted computer resource stored on the computer system, and execution of a remote application manager component on the computer system is also initiated. Under the control of the remote application manager component, the token is decrypted and a user is authenticated on the computer system using authentication information stored in the token. Whether the user is authorized to use the requested computer resource using authorization information stored in the token is then verified, as is whether the user has sufficient credit contained in the token to use the requested computer resource using credit information stored in the token. When the user is authenticated, authorized, and has sufficient credit, the requested computer resource is decrypted on the computer system and opened. Use of the computer resource is then monitored on the computer system to determine whether the user has sufficient credit to continue using the computer resource. A notification is provided when the monitored usage of the opened computer resource has exceeded the credit.

The disclosed embodiment provides the distinct advantage that it is usable in both continuous- and broken-connection modes of operations. That is to say that, the token may be used to verify and authenticate on the computer system in instances where an application executes on the user's computer system and where the user interacts with an application executing on a remote server.

Discussion of the Cited Reference

The system disclosed by Patel is substantially different from the embodiments disclosed by Applicants. In the system of Patel, authentication and verification of a token occur on a server rather than on a client computer system.

Patel discloses an application serving system in which a client system obtains an encrypted access token for a streamed application from a license server. Col. 2, lns. 50-52. The client system sends the encrypted access token to the server. Figure 22 ("Client sends token and Application file page identifiers"). The application server then validates the token to determine whether a client can access the streamed application. Figure 22 ("validate token" in box 2210); Col. 26, ln. 65 – Col. 27, ln. 13. ("The Application Server 2210 needs only to decrypt the Access Token (or a digest of it) via a secret key shared 2209 with the License Server 2205 (thus

verifying the Token is valid), then checking the validity of its contents, e.g., application identifier, and testing the expiration time.").

Patel does not perform any token validation or decryption based on a token at a client system. Patel further does not evaluate usage to determine whether a user has exceeded a credit limit on the client system. As noted above, all of these functions are performed on the server in the system of Patel. Patel provides no teaching or suggestion to do otherwise.

Discussion of the Claims

Turning now to the claims, the differences between the cited reference and the claimed invention will be pointed out. With respect to claim 1, Patel fails to teach or suggest, in combination with the other limitations of the claim, a method including the steps of "generating at a server a token containing encrypted user information including credit, authorization, and authentication information; transmitting the token to the computer system; transmitting a computer resource to the computer system, the computer resource being encrypted; *verifying at the computer system whether the user is authorized to use the requested computer resource using authorization information stored in the token; verifying at the computer system whether the user has sufficient credit contained in the token to use the requested computer resource using credit information stored in the token; when the user is authenticated, authorized, and has sufficient credit, decrypting and opening the requested computer resource at the computer system; monitoring the usage of the opened computer resource at the computer system to determine whether the user has sufficient credit to continue using the computer resource*." (emphasis added).

With respect to claim 11, Patel fails to teach or suggest, in combination with the other limitations of the claim, a method including the steps of "receiving from the server system, a token including encrypted information generated from the user information provided by the client system; a remote application manager component; and at least one computer resource, each computer resource being encrypted and the particular computer resources received being determined from the authorization information contained in the provided user information; *under control of the remote application manager component on the client system*, decrypting at the client system the token in response to a request to initiate execution of one of the computer

resources; authenticating the user of the client computer system; verifying whether the user is authorized to use the requested computer resource; verifying whether the user has sufficient credit contained in the token to use the requested computer resource; when the user is authenticated, authorized, and has sufficient credit, decrypting and initiating execution of the requested computer resource; and monitoring the usage of the executing computer resource and providing a notification when the monitored usage has exceeded the user's credit." (emphasis added).

With respect to claim 19, Patel fails to teach or suggest, in combination with the other limitations of the claim, a method including the steps of "generating a token including encrypted information generated from the user information provided by the client system; sending the token to the client system; sending a remote application manager component to the client system; sending at least one computer resource to the client system, each computer resource that is sent being encrypted; under control of the remote application manager component on the client system, initiating execution of the remote application manager component in response to a request to initiate execution of the computer resource; *decrypting at the client system the token and authenticating a user of the client computer system; verifying at the client system whether the user is authorized to use the computer resource; verifying at the client system whether the user has sufficient credit contained in the token to use the computer resource; when the user is authenticated, authorized, and has sufficient credit, decrypting and initiating execution of the computer resource; and, monitoring the usage of the executing computer resource at the client system and providing notification when the monitored usage has exceeded the user's credit*." (emphasis added).

With respect to claim 27, Patel fails to teach or suggest, in combination with the other limitations of the claim, a system including "a token component including encrypted user information, the user information including authentication, authorization, and credit information for a user of the client system; at least one computer resource component, each computer resource component being encrypted; a remote application manager component being adapted to receive the encrypted user information contained in the token, *the remote application manager component operable responsive to a request to open a computer resource component to decrypt*

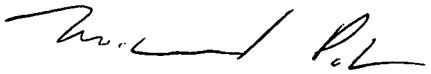
at the client system the encrypted user information, authenticate the user, determine whether the user is authorized to use the requested computer resource, and determine whether the user has sufficient credit to use the requested computer resource, the remote application manager component decrypting and opening the requested computer resource when the user is authenticated, authorized, and has sufficient credit, and monitoring the usage of the opened computer resource and providing a notification when the monitored usage has exceeded the user's credit." (emphasis added).

Claims 2-10, 12-18, 20-26, 28-30, are dependent on independent claims 1, 11, 19, and 27 respectively and are therefore allowable for at least the reasons discussed hereinabove.

All of the claims remaining in the application are now clearly allowable. Favorable consideration and a timely Notice of Allowance are earnestly solicited.

Respectfully submitted,

DORSEY & WHITNEY LLP



Michael G. Pate
Registration No. 53,439
Telephone No. (206) 903-2398

MGP:sp

Enclosures:
Postcard
Fee Transmittal Sheet (+ copy)

DORSEY & WHITNEY LLP
1420 Fifth Avenue, Suite 3400
Seattle, WA 98101-4010
(206) 903-8800 (telephone)
(206) 903-8820 (fax)

h:\ip\clients\micron technology\700\500767.01\500767.01 amend oa 030607.doc